ASSESSOR'S USER GUIDE*

Any opinions, findings, conclusions, or recommendations expressed in this publication and application do not necessarily reflect the views of FEMA. Additionally, neither FEMA or any of its employees makes any warrantee, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process included in this publication and application. Users of information from this publication and application assume all liability arising from such use.

INTRODUCTION

To support the building assessment process, this easy to use Risk Assessment Database application is provided with FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings.* The Risk Assessment Database is a standalone application that is both a collection tool and a management tool. Assessors can use the tool to assist in the systematic collection, storage, and reporting of assessment data. It has functions, folders, and displays to import and display threat matrices, digital photos, cost data, emergency plans, and certain Geographic Information System (GIS) products as part of the record of assessment. Managers can use the application to store, search, and analyze data collected from multiple assessments.

The Risk Assessment Database is initially installed on a desktop computer at an organization's headquarters. This database, referred to in this User Guide as the Manager's Database, becomes the main access and storage point for future assessment data. When an organization wants to conduct an assessment of a site or series of sites, a database administrator uses the application to produce a small temporary database, called the Assessor's Database, on a CD. Into this Assessor's Database are placed references, site plans, GIS portfolios, and other site-specific data that are known about the assessment site or are developed during the pre-assessment phase. This Assessor's Database is given to the Assessment Team and is loaded on one or more of their assessment computers (usually laptop computers). The Assessment Team then conducts their assessment and records information in the Assessor's Database. At the end of the assessment, the Assessment Team combines their data into one database and passes the files back to the database administrator. The administrator then loads the data into the Manager's Database for printing and analysis.

After initially installing the application, access to that Risk Assessment Database becomes restricted to only those designated users who have been assigned permission to access to the database by their administrator. Also, data can be viewed by all authorized users of the database, but changes to the data can only be made by those granted permission. All access permission questions should be directed to the database administrator of your organization.

The following are the hardware and software requirements for the Risk Assessment Database:

Pentium® 4 or equivalent processor
Windows XP
MS Access® 2002
256 MB of RAM recommended for all components

BEFORE THE ASSESSMENT: GETTING READY TO USE THE ASSESSOR'S VERSION OF THE RISK ASSESSMENT DATABASE

From your database administrator, the user should receive a folder named FEMA_452dB_Assessor containing the database application (3 files), assessment site(s) folder(s), which contain the folders,

and an application shortcut with the icon  or .

- The **FEMA_452dB_Assessor folder** must be copied to the **C:\ drive**; the database application is dependent on the folder being downloaded to this location on the computer.

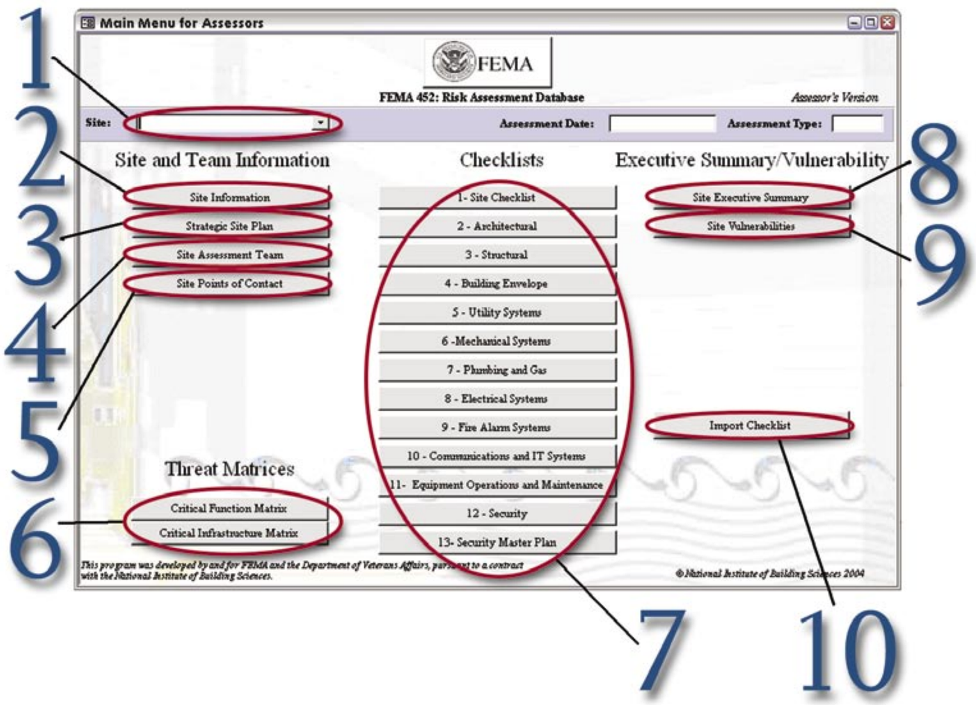
- The **application shortcut** should be copied to the **desktop**.

- When the user double clicks the application shortcut, the user receives a logon prompt:

- The user should log on using the user name and password provided by the database administrator.

- After logging in, the user will get the **Main Menu for Assessors**.

MAIN MENU



1. This is a drop down list of assessment sites. **An assessment site must be selected before any of the other buttons can be used.**

2. The ***Site Information*** button opens the **Site Information** report. This is not filled out by the on-site Assessor; it is usually completed during the assessment preparation period. If not pre-loaded, information can be collected and turned in to the Manager for inclusion after the on-site visit.

3. The ***Strategic Site Plan*** button opens the **Strategic Site Plan** in Microsoft Excel, if it is available. This is not filled out by the on-site Assessor; it is usually completed during the assessment preparation period. If not pre-loaded, information can be collected and turned in to the Manager for inclusion after the on-site visit.

4. The ***Site Assessment Team*** button opens the **Assessment Main Page** to the tab with information for the team that performed the assessment **(Assessment Team)**.

5. The ***Site Points of Contact*** button opens the **Assessment Main Page** to the tab with the contact information for the assessment site points of contact **(Points of Contact)**.

6. The ***Critical Function Matrix*** button opens the **Critical Functions Matrix**

form, and the ***Critical Infrastructures Matrix*** button opens the **Critical Infrastructures Matrix** form.

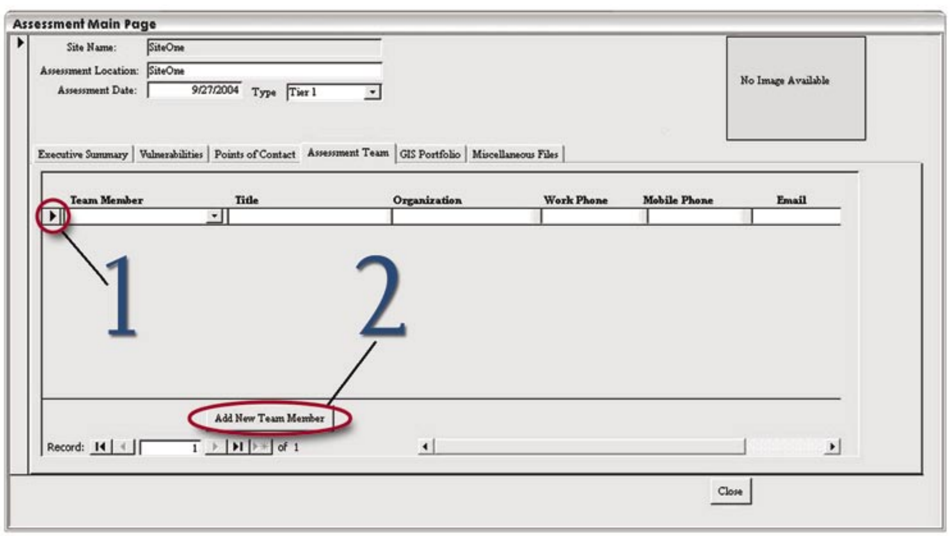
7. The ***Vulnerability Assessment Checklist*** buttons open a form that allows the user to input observations, recommendations/remediations, and vulnerability categorizations to the database for each checklist section. **(Observations and Recommendations/Remediations for Vulnerability Assessment Checklist Questions).**

8. The ***Site Executive Summary*** button opens the **Assessment Main Page** to the tab with the **Executive Summary**.

9. The ***Site Vulnerabilities*** button opens the **Assessment Main Page** to the tab with the **Vulnerabilities** for that assessment.

10. The Import Checklist button opens the **Select File** screen, which allows the main user to connect to another user's data for import.

Assessment Team

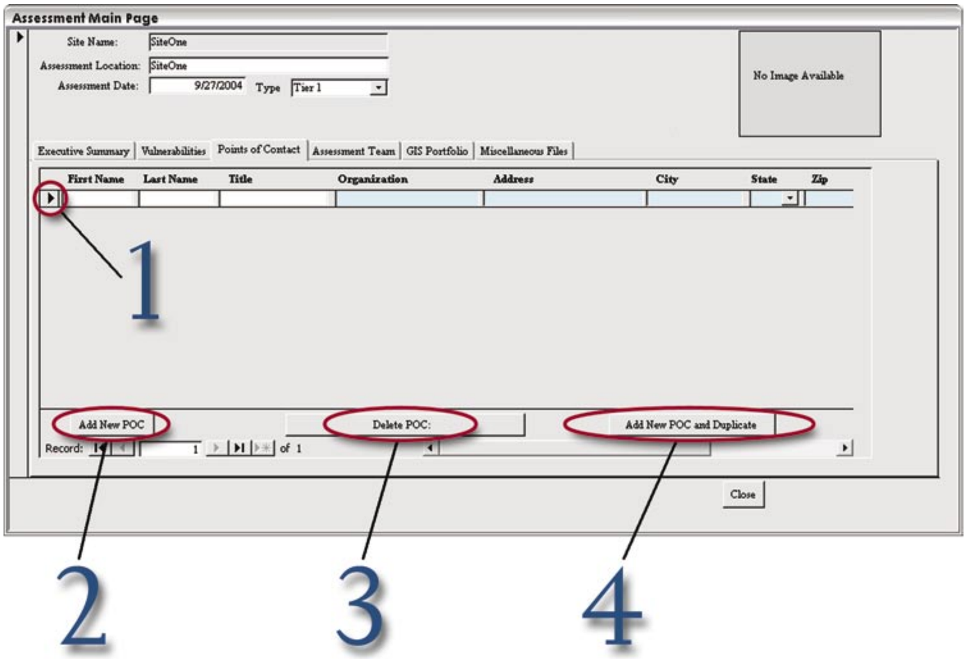


This form allows the user to enter information about Assessment Team members.

1. The black triangle indicates the record that is selected.

2. The ***Add New Team Member*** button allows for the creation of a new Assessment Team member for the assessment site designated in the upper left portion of this form.

Points of Contact



This form allows the user to enter information about points of contact (POC) at the assessment site.

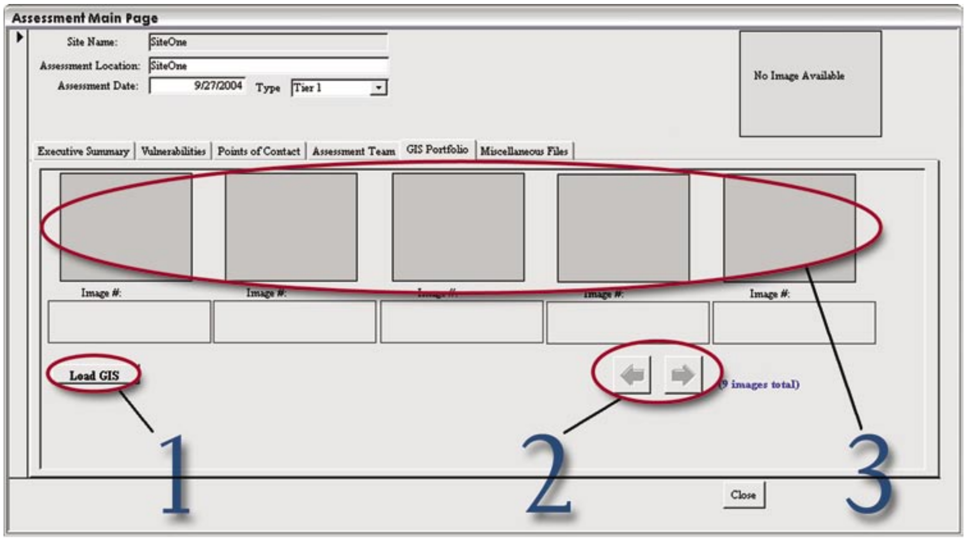
1. The black triangle indicates the record that is selected.

2. The ***Add New POC*** button allows for the creation of a new contact for the assessment site designated in the upper left portion of this form.

3. The **Delete POC** button allows the removal of the selected contact from the database.

4. The A***dd New POC and Duplicate*** button allows the creation of a new contact and duplicates the information in light blue in order to minimize data entry efforts.

GIS Portfolio



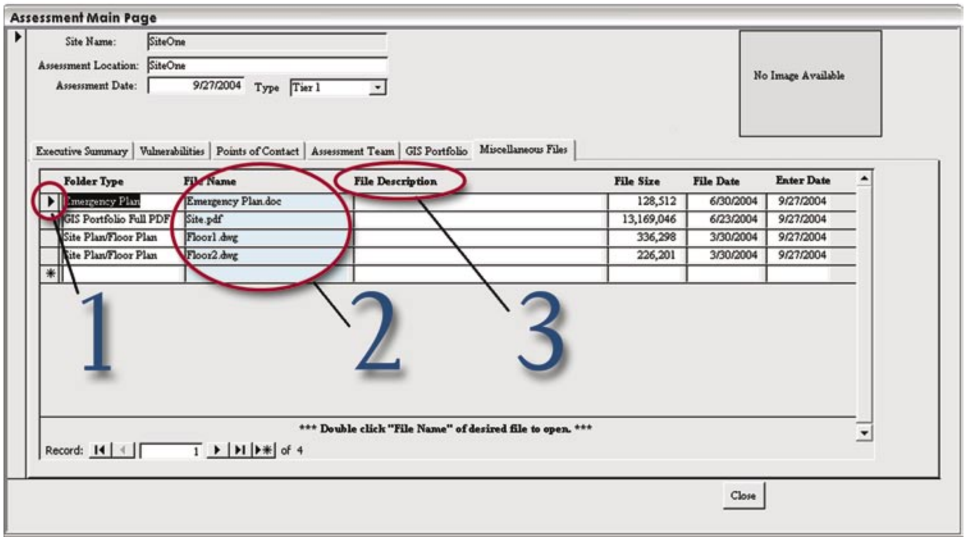
This form enables the user to see GIS images associated with the assessment site if developed during the pre-assessment period. These images are not entered by the on-site Assessor; the form is usually completed during the assessment preparation period. If not pre-loaded, information can be collected and turned in to the Manager for inclusion after the on-site visit.

1. The ***Load GIS*** button loads GIS images to the designated frames.

2. The 2 arrow button allows for navigation through pages of 5 GIS images, either to the previous 5 images or to the next 5 images.

3. Clicking on any of the GIS images will open the image in the ***Photo Zoom*** window, which displays the image larger, and the image can be printed individually in this window.

Miscellaneous Files



This form enables the user to see if files related to the assessment are available to view. (If developed during the pre-assessment period.) These images are not entered by the on-site Assessor; they are usually completed during the assessment preparation period. If not pre-loaded, information can be collected and turned in to the Manager for inclusion after the on-site visit.

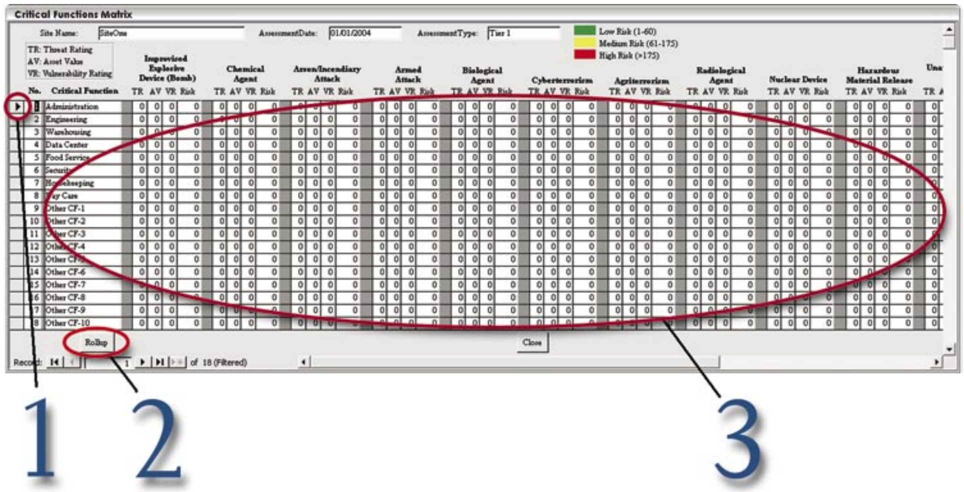
The form displays a list of the files available and allows the user to open and view the files.

1. The black triangle indicates the record that is selected.

2. Double-clicking any of the file names will open the associated file (examples of possible files to pre-load for the assessors include references, a GIS portfolio in PDF format, and/or past assessment reports).

3. The ***File Description*** field allows for descriptions to be typed in about each of the file names in the record.

CRITICAL FUNCTIONS MATRIX



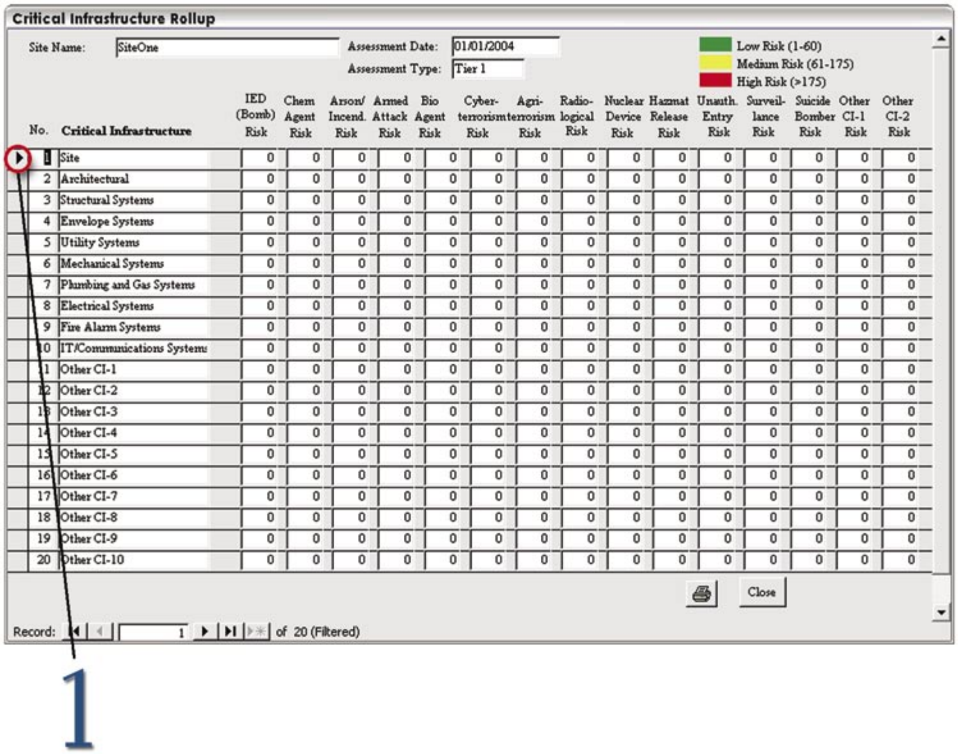
This form records and numerically displays the results of analysis performed during the assessment. The matrix lists Critical Functions down the left side and threats across the top to create Threat-pairs. For each Threat-pair, a numeric value, on a 1-10 scale, is recorded for a threat rating, an asset value rating, and a vulnerability rating. The methodology for determining the ratings is found in FEMA 452.

1. The black triangle indicates the record that is selected.

2. The ***Rollup*** button opens a window that summarizes all of the risk columns into one easy to read form called **Critical Functions Rollup.**

3. These fields are where values (1-10) are typed in for each of the Threat-pairs. The Risk Column is automatically generated and color coded.

Critical Functions Rollup



Critical Infrastructure Rollup

Site Name: SiteOne

Assessment Date: 01/01/2004

Assessment Type: Tier 1

Low Risk (1-60)
Medium Risk (61-175)
High Risk (>175)

No.	Critical Infrastructure	IED (Bomb) Risk	Chem Agent Risk	Arson/ Incend. Risk	Armed Attack Risk	Bio Agent Risk	Cyber-terrorism Risk	Agri-terrorism Risk	Radio-logical Risk	Nuclear Device Risk	Hazmat Release Risk	Unauth. Entry Risk	Surveil-lance Risk	Suicide Bomber Risk	Other CI-1 Risk	Other CI-2 Risk
1	Site	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Architectural	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	Structural Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	Envelope Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	Utility Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Mechanical Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	Plumbing and Gas Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	Electrical Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	Fire Alarm Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	IT/Communications Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	Other CI-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	Other CI-2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	Other CI-3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	Other CI-4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	Other CI-5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	Other CI-6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	Other CI-7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	Other CI-8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	Other CI-9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	Other CI-10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Close

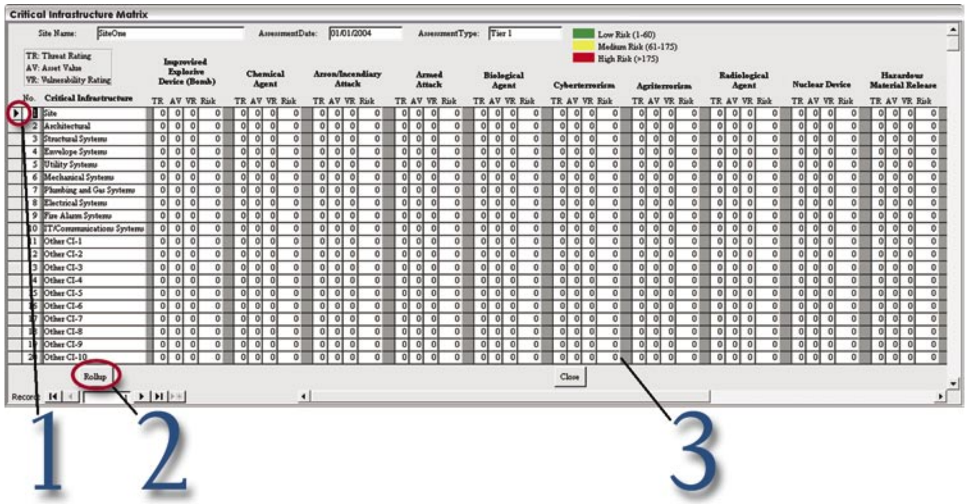
Record: 1 of 20 (Filtered)

1

This form displays a summary of the final numeric risk value of each Threat-pair in the **Critical Functions Matrix**.

1. The black triangle indicates the record that is selected.

CRITICAL INFRASTRUCTURE MATRIX



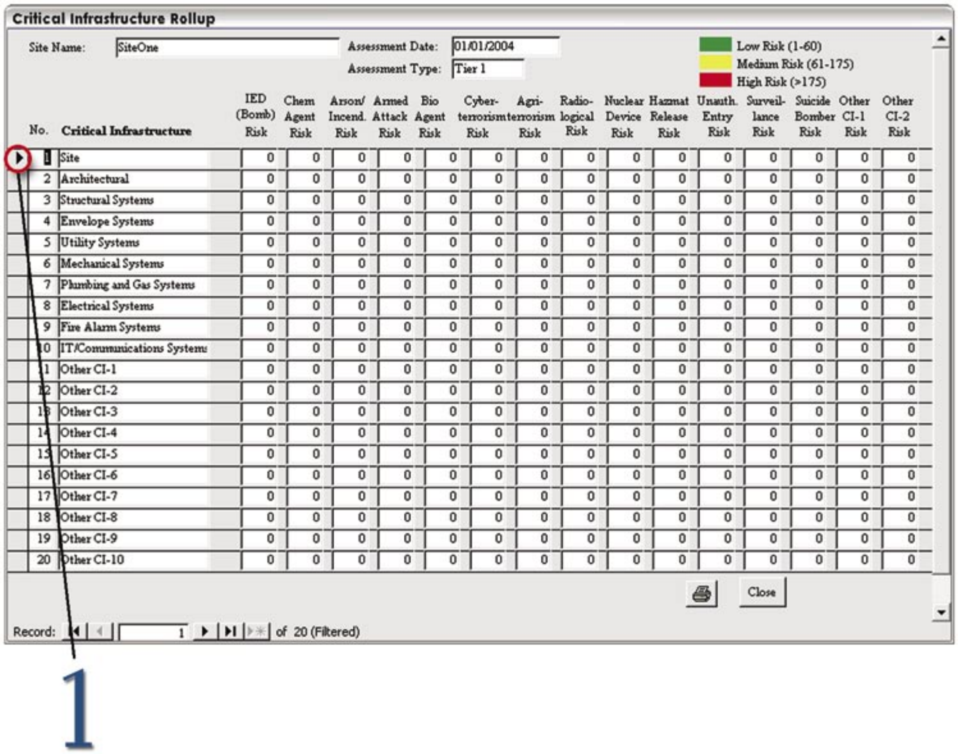
This form records and numerically displays the results of analysis performed during the assessment. The matrix lists Critical Infrastructure down the left side and threats across the top to create Threat-pairs. For each Threat-pair, a numeric value, on a 1-10 scale, is recorded for a threat rating, an asset value rating, and a vulnerability rating. The methodology for determining the ratings is found in FEMA 452.

1. The black triangle indicates the record that is selected.

2. The ***Rollup*** button opens a window that summarizes all of the risk columns into one easy to read called **Critical Infrastructure Rollup**.

3. These fields are where values (1-10) are typed in for each of the threats to a critical infrastructure.

Critical Infrastructure Rollup



Critical Infrastructure Rollup

Site Name: SiteOne

Assessment Date: 01/01/2004

Assessment Type: Tier 1

Low Risk (1-60)
Medium Risk (61-175)
High Risk (>175)

No.	Critical Infrastructure	IED (Bomb) Risk	Chem Agent Risk	Arson/ Incend. Risk	Armed Attack Risk	Bio Agent Risk	Cyber-terrorism Risk	Agri-terrorism Risk	Radio-logical Risk	Nuclear Device Risk	Hazmat Release Risk	Unauth. Entry Risk	Surveil-lance Risk	Suicide Bomber Risk	Other CI-1 Risk	Other CI-2 Risk
1	Site	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Architectural	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	Structural Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	Envelope Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	Utility Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Mechanical Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	Plumbing and Gas Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	Electrical Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	Fire Alarm Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	IT/Communications Systems	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	Other CI-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	Other CI-2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	Other CI-3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	Other CI-4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	Other CI-5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	Other CI-6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	Other CI-7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	Other CI-8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	Other CI-9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	Other CI-10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Close

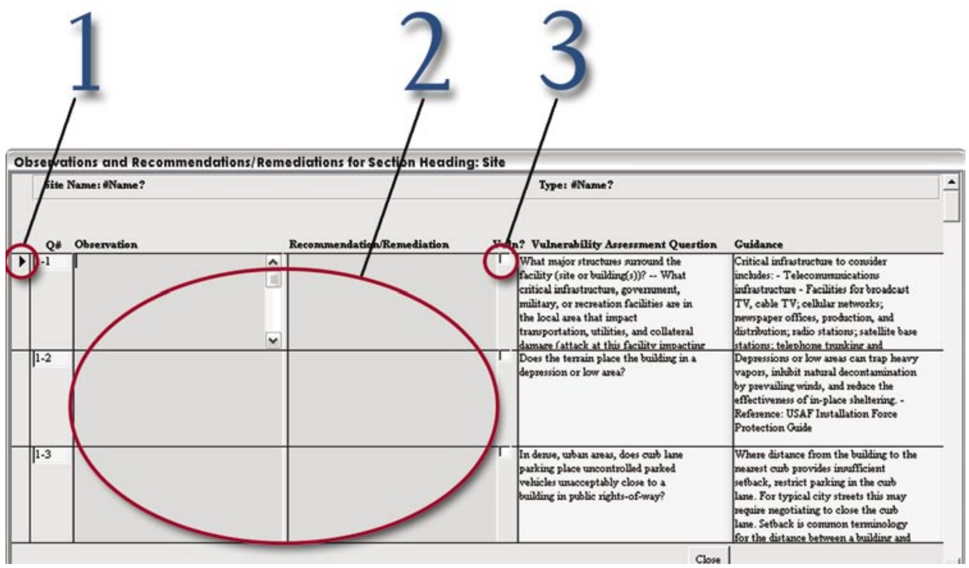
Record: 1 of 20 (Filtered)

1

This form is used to view the risk of threats for the specified critical infrastructure.

1. The black triangle indicates the record that is selected.

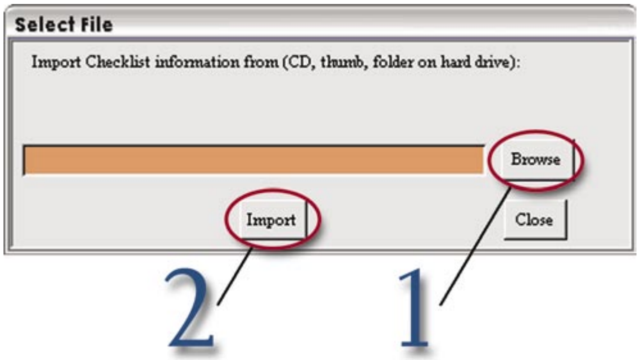
OBSERVATIONS AND RECOMMENDATIONS/ REMEDIATIONS FOR THE VULNERABILITY ASSESSMENT CHECKLIST SECTIONS



This form allows the user to enter observations and recommendations/remediations for each of the vulnerability assessment checklist questions.

1. The black triangle indicates the record that is selected.
2. These fields are where observations and recommendations/remediations are entered by the user.
3. This checkbox is selected if the observation is a vulnerability; the observations and recommendations/remediations are copied to the **Vulnerabilities** page.

SELECT FILE



If assessment data are collected and recorded on more than one computer, this form allows the "main user" to connect to another user's database, and import the other user's data. Note: the threat matrices cannot be imported, so it is important for the "main user" to have the threat matrices data in their database.

1. The ***Browse*** button allows the user to search for and select another database to connect to. (Note: The database to connect to will have "Data" in its name, not "Application.")

2. The ***Import*** button allows the user to connect the database selected in 1.

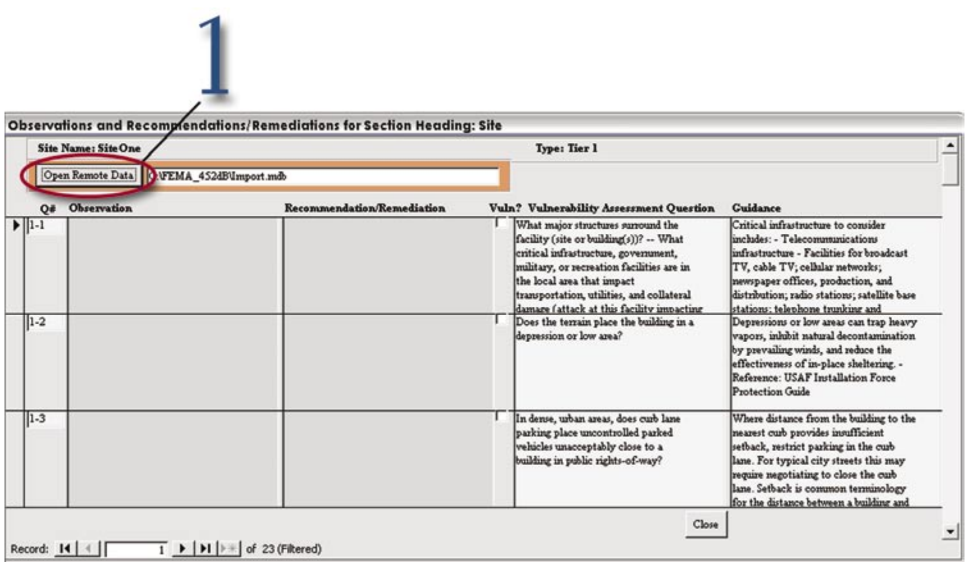
Once a connection is made, this window will pop up. Simply click the ***OK*** button to make the data available for viewing or copying.

IMPORTING DATA FROM OTHER DATABASES

After a database connection has been made (see **Select File**), the user can start importing another user's data.

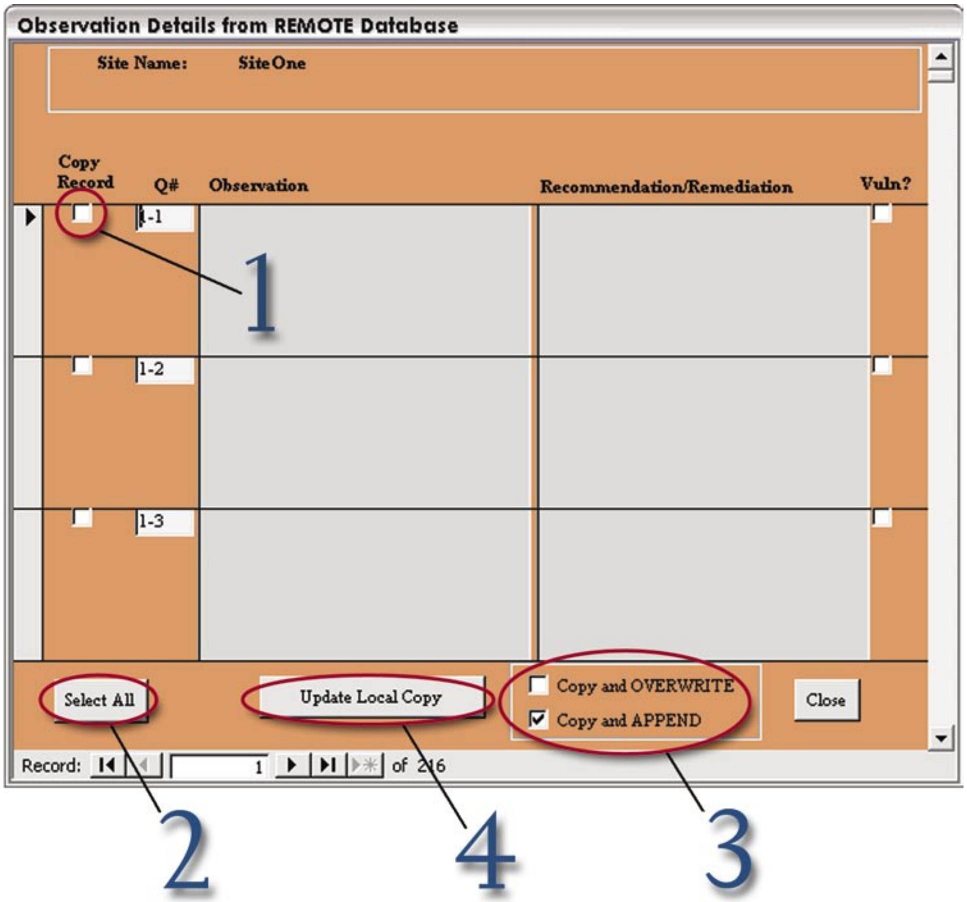
Importing Observation and Recommendation/ Remediation Data

Once connected to another database, the **Main Menu** screen will appear the same. Clicking on any of the Vulnerability Assessment Checklist buttons will supply this window with a new ***Open Remote Data*** button added to the screen.



1. The ***Open Remote Data*** button will make the additional data available and open the **Observation Details from REMOTE Database** screen.

Observation Details from the REMOTE Database



This form displays the remote data and allows the Main User to choose which data to import.

1. This checkbox allows the user to select individual records to be imported.

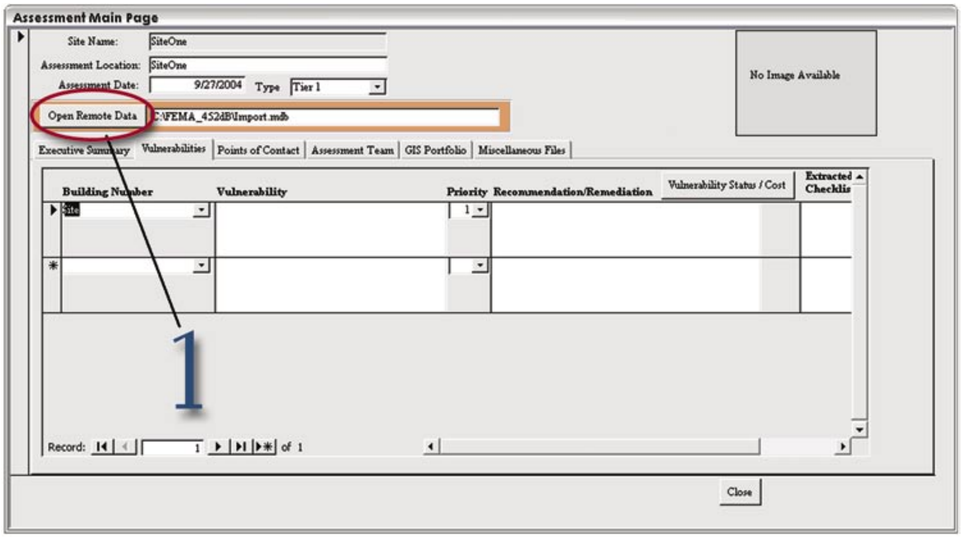
2. The ***Select All*** button selects all of the records.

3. These checkboxes are options for copying another user's data. The ***Copy and OVERWRITE*** checkbox will overwrite the data in the user's database; the ***Copy and APPEND*** checkbox will add the other user's data to the data existing in the user's database.

4. The ***Update Local Copy*** button is the final step and copies the data into the main user's database

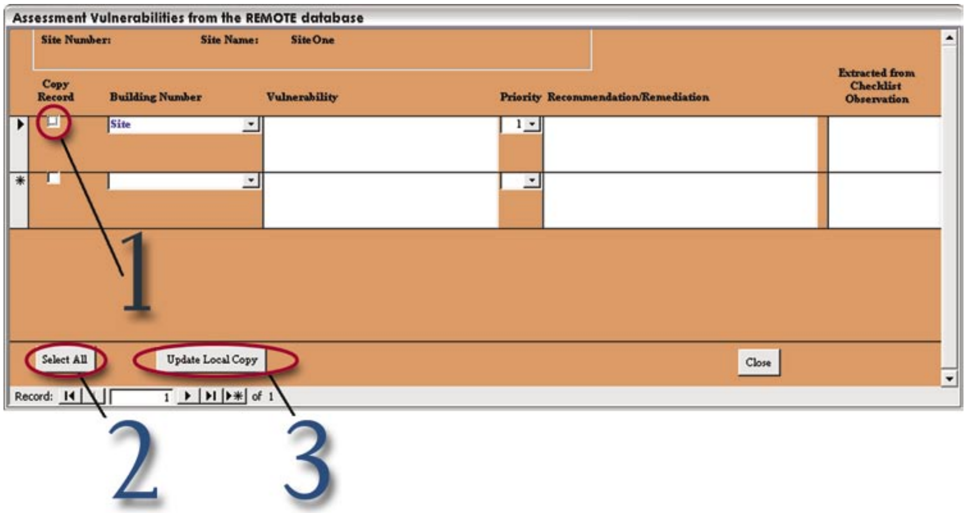
Importing Vulnerability and Recommendation/ Remediation Data

Once connected to another database, the **Main Menu** screen will appear the same. Clicking on the ***Site Vulnerabilities*** button will supply this window with a new ***Open Remote Data*** button added to the screen.



1. The ***Open Remote Data*** button will make the additional data available and open the **Observation Details from REMOTE Database** screen.

Assessment Vulnerabilities from the REMOTE Database



This form displays the remote data and allows the main user to choose which data to import.

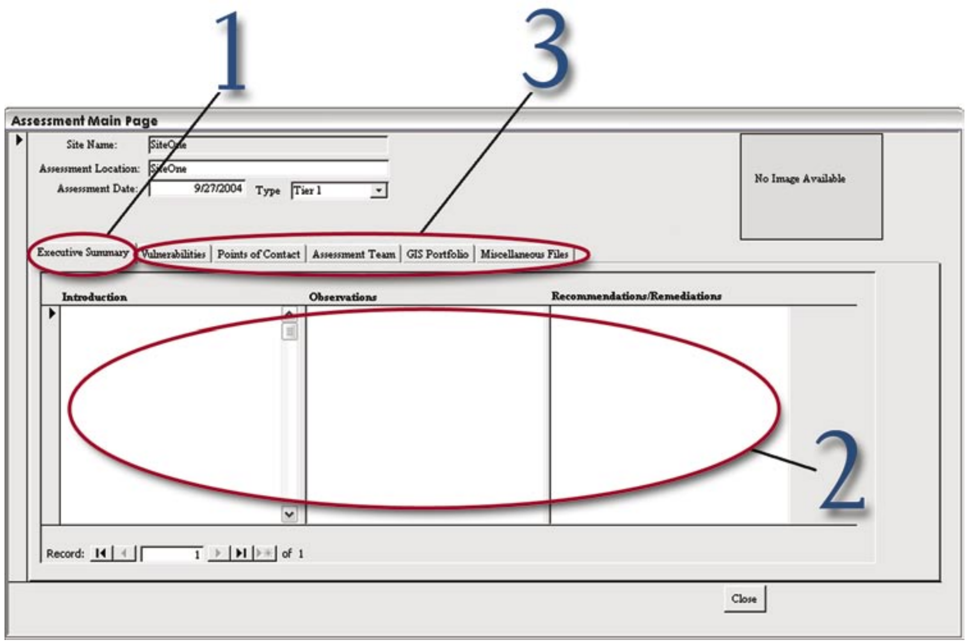
1. This checkbox allows the user to select individual records to be imported.

2. The ***Select All*** button selects all the records.

3. The ***Update Local Copy*** button is the final step and copies the data into the main user's database.

ASSESSMENT MAIN PAGE

Executive Summary



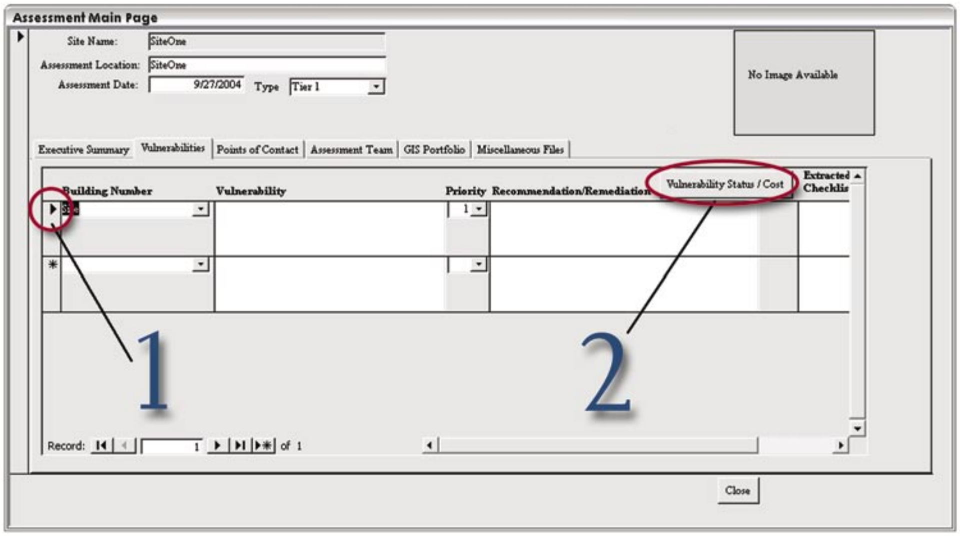
This form allows the user to enter an **Executive Summary** for the assessment site report.

1. The first tab is the **Executive Summary** input form for the site selected in the drop down list on the **Main Menu**.

2. This information is the first three paragraphs of the final assessment report and usually contains broad over arching information. Individual details are usually listed later in the vulnerability section of the report.

3. The page also allows users to navigate to other forms in the database without having to return to the main screen as follows:

Vulnerabilities

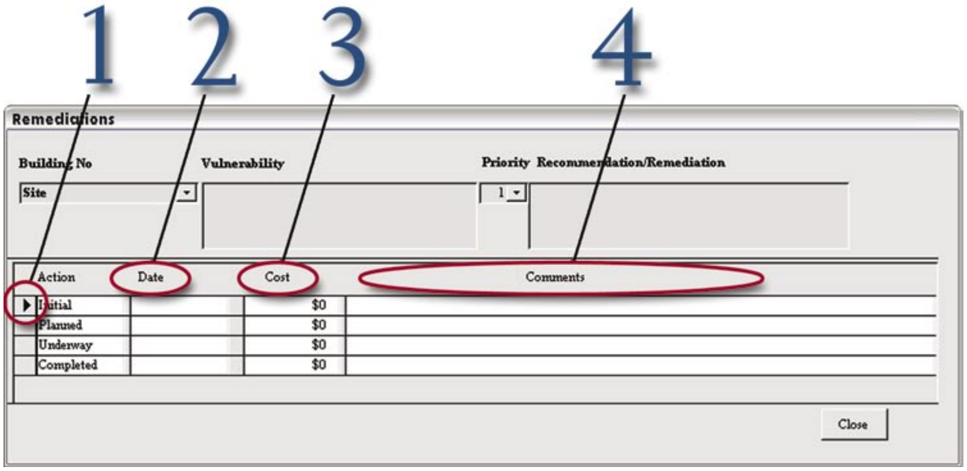


This form allows the user to enter additional information on the vulnerabilities and recommendations/remediations observed while performing the assessment. The form is linked to the **Observations and Recommendation/Remediation** form. Observations that were previously identified and "checked" as a vulnerability are automatically loaded into this form. These vulnerabilities should now be furthered analyzed and assigned a priority, a location, and a remediation cost estimate. (Note: Priority and Building Number are required.)

1. The black triangle indicates the record that is selected.

2. The ***Project Status/Cost*** button opens the **Remediations** form.

Remediations



This form allows the user to enter any remediation information related to an observed vulnerability, including date, cost, and comments.

1. The black triangle indicates the record that is selected.

2. This date field can be filled in by the user to keep the remediation cost records up to date.

3. Enter the cost for the remediation into this field to keep the remediation records up to date.

4. Enter any comments for the remediation in this field.

AFTER THE ASSESSMENT: GIVING DATA TO THE DATABASE ADMINISTRATOR

All of the assessment data should be in **one database**, the "main user's."

1. Once the database is complete, make sure all of the files are in the proper folder locations for each of the assessment site folders in the FEMA_452dB_Assessor folder. (Photos in the Photos folder, digital floor plans (such as CADD) in the Site_and_Floorplans folder, and emergency management plans in the Emergency_Plans folder.)

2. Provide the database administrator with a database file containing the word "Data," the Photos folder, the Site_and_Floorplans folder, and the Emergency_Plans folder.